EXHIBIT 3

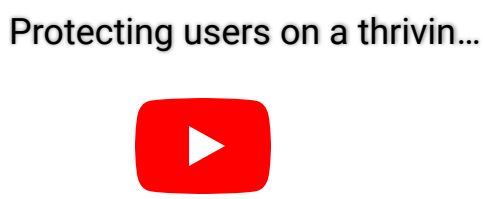
What is the Privacy Sandbox?

The Privacy Sandbox initiative aims to create technologies that both protect people's privacy online and give companies and developers tools to build thriving digital businesses.

The Privacy Sandbox has two core aims:

- Phase out support for third-party cookies when new solutions are in place.
- Reduce cross-site and cross-app tracking while helping to keep online content and services free for all.

The Privacy Sandbox APIs require web browsers to take on a new role. Rather than working with limited tools and protections, the APIs allow a user's browser to act on the user's behalf—locally, on their device—to protect the user's identifying information as they navigate the web. This is a shift in direction for browsers.



The Privacy Sandbox's vision of the future has browsers providing specific tools to satisfy specific use cases, while preserving user privacy.

What are the Privacy Sandbox proposals?

Chrome and other ecosystem stakeholders have offered more than 30 proposals to date, which can be found in the public resources of W3C groups (https://github.com/w3c/web-advertising#ideas-and-proposals-links-outside-this-repo). These proposals cover a wide variety of use cases and requirements.

Proposals have a lifecycle with up to three phases before becoming web standards (https://www.w3.org/standards/): discussion, testing, and scaled adoption. It's critical that we receive feedback (/privacy-sandbox/setup/web/feedback) from developers and industry leaders to ensure we create durable web features with broad utility and robust privacy protections for users. Read more about the proposal lifecycle (/privacy-sandbox/overview/proposal-lifecycle).

Several key proposals are listed below.

Strengthen cross-site privacy boundaries

- **CHIPS** (/privacy-sandbox/3pcd/chips): Allow developers to opt-in a cookie to partitioned storage, with a separate cookie jar per top-level site.
- **Related Website Sets** (/privacy-sandbox/3pcd/related-website-sets): Allow related domain names owned by the same entity to declare themselves as belonging to the same first party.
- **Shared Storage** (/privacy-sandbox/relevance/shared-storage): Create a general-purpose API which allows sites to store and access unpartitioned cross-site data. This data must be read in a secure environment to prevent leakage.
- **Storage Partitioning** (/privacy-sandbox/3pcd/storage-partitioning): Enable all forms of user agent state (https://github.com/privacycg/storage-partitioning#user-agent-state), such as `localStorage` or cookies, to be double-keyed: by the top-level site as well as the origin of the resource being loaded, rather than a single origin or site.
- **Fenced Frames** (/privacy-sandbox/relevance/fenced-frame): Securely embed content onto a page without sharing cross-site data.
- **Network State Partitioning** (https://github.com/MattMenke2/Explainer---Partition-Network-State): Prevent browser network resources being shared across first-party contexts, by ensuring that every request has a network partition key that must match in order for resources to be reused.
- **Federated Credential Management (FedCM)** (/privacy-sandbox/3pcd/fedcm): Support federated identity without sharing the user's email address or other identifying information with a third-party service or website, unless the user explicitly agrees to do so.

Show relevant content and ads

- **Topics API** (/privacy-sandbox/relevance/topics): Enable interest-based advertising without use of third-party cookies or tracking user behavior across sites.
- **Protected Audience API** (/privacy-sandbox/relevance/protected-audience): Ad selection to serve remarketing and custom audience use cases, designed so that it cannot be used by third parties to track user browsing behavior across sites. The Protected Audience API is the first experiment to be implemented in Chromium from the TURTLEDOVE (https://github.com/WICG/turtledove) family of proposals.

Measure digital ads

- **Attribution Reporting** (/privacy-sandbox/relevance/attribution-reporting): Correlate ad clicks or ad views with conversions. Ad techs can generate event-level or summary reports (/privacy-sandbox/relevance/attribution-reporting/summary-reports).
- **Private Aggregation API** (/privacy-sandbox/relevance/private-aggregation): Generate noisy summary reports with cross-site data.

Prevent covert tracking

- **User-Agent reduction and User-Agent Client Hints** (/privacy-sandbox/protections/user-agent): Limit passively shared browser data to reduce the volume of sensitive information which leads to fingerprinting. Client Hints allow developers to actively request only the information they need about the user's device or conditions.
- **IP Protection** (/privacy-sandbox/protections/ip-protection): Improve user privacy by protecting their IP address from being used for tracking.
- **Bounce tracking mitigations** (/privacy-sandbox/protections/bounce-tracking-mitigations): A proposal to reduce or eliminate the ability of bounce tracking to recognize people across contexts.
- **Privacy Budget** (/privacy-sandbox/protections/privacy-budget): Limit the amount of individual user data exposed to sites to prevent covert tracking.

Fight spam and fraud on the web

- **Private State Tokens** (/privacy-sandbox/protections/private-state-tokens): Allow websites to convey a limited amount of information from one browsing context to another (for example, across sites) to help combat fraud, without passive tracking.

Engage and share feedback

- **GitHub**: read the explainers on GitHub and raise questions or comments in the Issues tab for each.
- **W3C**: Use cases can be discussed and industry feedback shared in the W3C Improving Web Advertising Business Group (https://www.w3.org/community/web-adv/), the Privacy

Community Group (https://www.w3.org/community/privacycg/participants), and the Web Incubator Community Group (https://github.com/WICG).

- **Developer support**: Ask questions and join discussions on the Privacy Sandbox Developer Support repo (https://github.com/GoogleChromeLabs/privacy-sandbox-dev-support).

Find out more

- Digging into the Privacy Sandbox (https://web.dev/digging-into-the-privacy-sandbox)
- A Potential Privacy Model for the Web (https://github.com/michaelkleber/privacy-model) sets out the core principles underlying the APIs.
- Chromium's overview of the Privacy Sandbox (https://www.chromium.org/Home/chromium-privacy/privacy-sandbox)
- Google AI Blog: Federated Learning: Collaborative Machine Learning without Centralized Training Data (https://ai.googleblog.com/2017/04/federated-learning-collaborative.html)
- The future of third-party cookies (https://blog.chromium.org/2019/10/developers-get-ready-for-new.html)

Stay up to date on the progress of the Privacy Sandbox

You can follow the monthly updates to the Privacy Sandbox in our blog (/privacy-sandbox/blog).

The Privacy Sandbox timeline (https://privacysandbox.com/timeline/) shows the current status and schedule for proposals.

These high-level resources will provide signposts to changes across the project, but for individual proposals where you want to follow in detail you should:

- Watch or Star proposal repos on GitHub to get notification of new issues and updates: the Privacy Sandbox status page (/privacy-sandbox/overview/status) provides a link to the repository for each proposal
- Join the associated W3C group (https://www.w3.org/groups/) for regular meetings discussing the proposal detail
- Star the associated entry on Chrome Platform Status (https://chromestatus.com) for email updates on Chrome implementation changes.

Get involved

- Participate in incubation, testing and refinement of the APIs: How to participate in the Privacy Sandbox initiative (/privacy-sandbox/blog/privacy-sandbox-participate)
- As a developer, join discussions or ask questions: Privacy Sandbox Developer Support (https://github.com/GoogleChromeLabs/privacy-sandbox-dev-support)

For questions about specific APIs, you can file an issue on the GitHub repository for an API Explainer (/privacy-sandbox/overview/status).

Last updated 2024-03-07 UTC.